CWSP-206.VCEplus.premium.exam.60q

Number: CWSP-206
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

CWSP-206

CWSP Certified Wireless Security Professional

Version 1.0

Exam A

QUESTION 1
You have a Windows laptop computer with an integrated, dual-band, Wi-Fi compliant adapter. Your laptop computer has protocol analyzer software installed that is capable of capturing and decoding 802.11ac data. What statement best describes the likely ability to capture 802.11ac frames for security testing purposes?

A. Integrated 802.11ac adapters are not typically compatible with protocol analyzers in Windows laptops. It is often best to use a USB adapter or carefully select a laptop with an integrated adapter that will work.
B. Laptops cannot be used to capture 802.11ac frames because they do not support MU-MIMO.
C. Only Wireshark can be used to capture 802.11ac frames as no other protocol analyzer has implemented the proper frame decodes.
D. All integrated 802.11ac adapters will work with most protocol analyzers for frame capture, including the Radio Tap Header.
E. The only method available to capture 802.11ac frames is to perform a remote capture with a compatible access point.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
In order to acquire credentials of a valid user on a public hotspot network, what attacks may be conducted? Choose the single completely correct answer.

A. MAC denial of service and/or physical theft
B. Social engineering and/or eavesdropping
C. Authentication cracking and/or RF DoS
D. Code injection and/or XSS
E. RF DoS and/or physical theft

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3 What WLAN client device behavior is exploited by an attacker during a hijacking attack?

A. After the initial association and 4-way handshake, client stations and access points do not need to perform another 4-way handshake, even if connectivity is lost.
B. Client drivers scan for and connect to access point in the 2.4 GHz band before scanning the 5 GHz band.
C. When the RF signal between a client and an access point is disrupted for more than a few seconds, the client device will attempt to associate to an access point with better signal quality.
D. When the RF signal between a client and an access point is lost, the client will not seek to reassociate with another access point until the 120 second hold down timer has expired.
E. As specified by the Wi-Fi Alliance, clients using Open System authentication must allow direct client-to-client connections, even in an infrastructure BSS.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
What software and hardware tools are used in the process performed to hijack a wireless station from the authorized wireless network onto an unauthorized wireless network?

A. A low-gain patch antenna and terminal emulation software
B. MAC spoofing software and MAC DoS software
C. RF jamming device and a wireless radio card

D. A wireless workgroup bridge and a protocol analyzer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Many computer users connect to the Internet at airports, which often have 802.11n access points with a captive portal for authentication. While using an airport hotspot with this security solution, to what type of wireless attack is a user susceptible?

A. Wi-Fi phishing
B. Management interface exploits
C. UDP port redirection
D. IGMP snooping

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
During 802.1X/LEAP authentication, the username is passed across the wireless medium in clear text. From a security perspective, why is this significant?

A. The username can be looked up in a dictionary file that lists common username/password combinations.
B. The username is needed for Personal Access Credential (PAC) and X.509 certificate validation.
C. 4-Way Handshake nonces are based on the username in WPA and WPA2 authentication.
D. The username is an input to the LEAP challenge/response hash that is exploited, so the username must be known to conduct authentication cracking.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
In XYZ's small business, two autonomous 802.11ac APs and 12 client devices are in use with WPA2-Personal. What statement about the WLAN security of this company is true?

A. Intruders may obtain the passphrase with an offline dictionary attack and gain network access, but will be unable to decrypt the data traffic of other users.
B. Because WPA2-Personal uses Open System authentication followed by a 4-Way Handshake, hijacking attacks are easily performed.
C. A successful attack against all unicast traffic on the network would require a weak passphrase dictionary attack and the capture of the latest 4-Way Handshake for each client.
D. An unauthorized wireless client device cannot associate, but can eavesdrop on some data because WPA2-Personal does not encrypt multicast or broadcast traffic.
E. An unauthorized WLAN user with a protocol analyzer can decode data frames of authorized users if he captures the BSSID, client MAC address, and a user's 4-Way Handshake.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8

The Aircrack-ng WLAN software tool can capture and transmit modified 802.11 frames over the wireless network. It comes pre-installed on Kali Linux and some other Linux distributions. Which one of the following would not be a suitable penetration testing action taken with this tool?

A. Auditing the configuration and functionality of a WIPS by simulating common attack sequences.
B. Transmitting a deauthentication frame to disconnect a user from the AP.
C. Cracking the authentication or encryption processes implemented poorly in some WLANs.
D. Probing the RADIUS server and authenticator to expose the RADIUS shared secret.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
You manage a wireless network that services 200 wireless users. Your facility requires 20 access points, and you have installed an IEEE 802.11-compliant implementation of 802.1X/LEAP with AES-CCMP as an authentication and encryption solution. In this configuration, the wireless network is initially susceptible to what type of attack?

A. Offline dictionary attacks
B. Application eavesdropping
C. Session hijacking
D. Layer 3 peer-to-peer
E. Encryption cracking

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
ABC Corporation is evaluating the security solution for their existing WLAN. Two of their supported solutions include a PPTP VPN and 802.1X/LEAP. They have used PPTP VPNs because of their wide support in server and desktop operating systems. While both PPTP and LEAP adhere to the minimum requirements of the corporate security policy, some individuals have raised concerns about MS-CHAPv2 (and similar) authentication and the known fact that MSCHAPv2 has proven vulnerable in improper implementations. As a consultant, what do you tell ABC Corporation about implementing MS-CHAPv2 authentication?

A. MS-CHAPv2 is only appropriate for WLAN security when used inside a TLS-encrypted tunnel.
B. When implemented with AES-CCMP encryption, MS-CHAPv2 is very secure.
C. MS-CHAPv2 uses AES authentication, and is therefore secure.
D. MS-CHAPv2 is compliant with WPA-Personal, but not WPA2-Enterprise.
E. LEAP's use of MS-CHAPv2 is only secure when combined with WEP.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
You perform a protocol capture using Wireshark and a compatible 802.11 adapter in Linux. When viewing the capture, you see an auth req frame and an auth rsp frame. Then you see an assoc req frame and an assoc rsp frame. Shortly after, you see DHCP communications and then ISAKMP protocol packets. What security solution is represented?

A. 802.1X/EAP-TTLS
B. WPA2-Personal with AES-CCMP
C. 802.1X/PEAPv0/MS-CHAPv2
D. EAP-MD5

E. Open 802.11 authentication with IPSec

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
In a security penetration exercise, a WLAN consultant obtains the WEP key of XYZ Corporation's wireless network. Demonstrating the vulnerabilities of using WEP, the consultant uses a laptop running a software AP in an attempt to hijack the authorized user's connections. XYZ's legacy network is using 802.11n APs with 802.11b, 11g, and 11n client devices. With this setup, how can the consultant cause all of the authorized clients to establish Layer 2 connectivity with the software access point?

A. When the RF signal between the clients and the authorized AP is temporarily disrupted and the consultant's software AP is using the same SSID on a different channel than the authorized AP, the clients will reassociate to the softwareAP.
B. If the consultant's software AP broadcasts Beacon frames that advertise 802.11g data rates that are faster rates than XYZ's current 802.11b data rates, all WLAN clients will reassociate to the faster AP.
C. A higher SSID priority value configured in the Beacon frames of the consultant's software AP will take priority over the SSID in the authorized AP, causing the clients to reassociate.
D. All WLAN clients will reassociate to the consultant's software AP if the consultant's software AP provides the same SSID on any channel with a 10 dB SNR improvement over the authorized AP.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
As the primary security engineer for a large corporate network, you have been asked to author a new security policy for the wireless network. While most client devices support 802.1X authentication, some legacy devices still only support passphrase/PSK-based security methods. When writing the 802.11 security policy, what password-related items should be addressed?

A. Certificates should always be recommended instead of passwords for 802.11 client authentication.
B. Password complexity should be maximized so that weak WEP IV attacks are prevented.
C. Static passwords should be changed on a regular basis to minimize the vulnerabilities of a PSK-based authentication.
D. EAP-TLS must be implemented in such scenarios.
E. MS-CHAPv2 passwords used with EAP/PEAPv0 should be stronger than typical WPA2-PSK passphrases.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14 ABC Hospital wishes to create a strong security policy as a first step in securing their 802.11 WLAN. Before creating the WLAN security policy, what should you ensure you possess?

A. Management support for the process.
B. Security policy generation software.
C. End-user training manuals for the policies to be created.
D. Awareness of the exact vendor devices being installed.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15

What policy would help mitigate the impact of peer-to-peer attacks against wireless-enabled corporate laptop computers when the laptops are also used on public access networks such as wireless hotspots?

A. Require Port Address Translation (PAT) on each laptop.
B. Require secure applications such as POP, HTTP, and SSH.
C. Require VPN software for connectivity to the corporate network.
D. Require WPA2-Enterprise as the minimal WLAN security solution.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16 What EAP type supports using MS-CHAPv2, EAP-GTC or EAP-TLS for wireless client authentication?

A. EAP-GTC
B. PEAP
C. EAP-TTLS
D. LEAP
E. H-REAP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
You must implement 7 APs for a branch office location in your organizations. All APs will be autonomous and provide the same two SSIDs (CORP1879 and Guest).

Because each AP is managed directly through a web-based interface, what must be changed on every AP before enabling the WLANs to ensure proper staging procedures are followed?

A. Output power
B. Fragmentation threshold
C. Administrative password
D. Cell radius

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
You are installing 6 APs on the outside of your facility. They will be mounted at a height of 6 feet. What must you do to implement these APs in a secure manner beyond the normal indoor AP implementations? (Choose the single best answer.)

A. Ensure proper physical and environmental security using outdoor ruggedized APs or enclosures.
B. Use internal antennas.
C. Use external antennas.
D. Power the APs using PoE.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Fred works primarily from home and public wireless hotspots rather than commuting to office. He frequently accesses the office network remotely from his Mac laptop using the local 802.11 WLAN. In this remote scenario, what single wireless security practice will provide the greatest security for Fred?

A. Use enterprise WIPS on the corporate office network.
B. Use 802.1X/PEAPv0 to connect to the corporate office network from public hotspots.
C. Use secure protocols, such as FTP, for remote file transfers.
D. Use an IPSec VPN for connectivity to the office network.
E. Use only HTTPS when agreeing to acceptable use terms on public networks.
F. Use WIPS sensor software on the laptop to monitor for risks and attacks.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Which one of the following is not a role defined in the 802.1X authentication procedures used in 802.11 and 802.3 networks for port-based authentication?

A. AAA Server
B. Authentication Server
C. Supplicant
D. Authenticator

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21 What TKIP feature was introduced to counter the weak integrity check algorithm used in WEP?

A. RC5 stream cipher
B. Block cipher support
C. Sequence counters
D. 32-bit ICV (CRC-32)
E. Michael

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22 Which of the following is a valid reason to avoid the use of EAP-MD5 in production WLANs? A. It does not support a RADIUS server.

B. It is not a valid EAP type.
C. It does not support mutual authentication.
D. It does not support the outer identity.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Your organization is using EAP as an authentication framework with a specific type that meets the requirements of your corporate policies. Which one of the following statements is true related to this implementation?

A. The client STAs may communicate over the controlled port in order to authenticate as soon as the Open System authentication completes.
B. The client STAs may communicate over the uncontrolled port in order to authenticate as soon as the Open System authentication completes.
C. The client STAs may use a different, but complementary, EAP type than the AP STAs.
D. The client will be the authenticator in this scenario.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
A WLAN consultant has just finished installing a WLAN controller with 15 controller-based APs. Two SSIDs with separate VLANs are configured for this network, and both VLANs are configured to use the same RADIUS server. The SSIDs are configured as follows:

1. SSID Blue – VLAN 10 – Lightweight EAP (LEAP) authentication – CCMP cipher suite
2. SSID Red – VLAN 20 – PEAPv0/EAP-TLS authentication – TKIP cipher suite

The consultant's computer can successfully authenticate and browse the Internet when using the Blue SSID. The same computer cannot authenticate when using the Red SSID. What is a possible cause of the problem?

A. The consultant does not have a valid Kerberos ID on the Blue VLAN.
B. The client does not have a proper certificate installed for the tunneled authentication within the established TLS tunnel.
C. The TKIP cipher suite is not a valid option for PEAPv0 authentication.
D. The Red VLAN does not use server certificate, but the client requires one.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Your network implements an 802.1X/EAP-based wireless security solution. A WLAN controller is installed and manages seven APs. FreeRADIUS is used for the RADIUS server and is installed on a dedicated server named SRV21. One example client is a MacBook Pro with 8 GB RAM. What device functions as the 802.1X/EAP Authenticator?

A. WLAN Controller/AP
B. MacBook Pro
C. SRV21
D. RADIUS server

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
In an IEEE 802.11-compliant WLAN, when is the 802.1X Controlled Port placed into the unblocked state?

A. After EAP authentication is successful
B. After Open System authentication
C. After the 4-Way Handshake
D. After any Group Handshake

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
When using a tunneled EAP type, such as PEAP, what component is protected inside the TLS tunnel so that it is not sent in clear text across the wireless medium?

A. Server credentials
B. User credentials
C. RADIUS shared secret
D. X.509 certificates

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28 What protocol, listed here, allows a network manager to securely administer the network?

A. TFTP
B. Telnet
C. HTTPS
D. SNMPv2

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
XYZ Company has recently installed a controller-based WLAN and is using a RADIUS server to query authentication requests to an LDAP server. XYZ maintains user-based access policies and would like to use the RADIUS server to facilitate network authorization. What RADIUS feature could be used by XYZ to assign the proper network permissions to users during authentications?

A. RADIUS can reassign a client's 802.11 association to a new SSID by referencing a username-to-SSID mapping table in the LDAP user database.
B. The RADIUS server can support vendor-specific attributes in the ACCESS-ACCEPT response, which can be used for user policy assignment.
C. The RADIUS server can communicate with the DHCP server to issue the appropriate IP address and VLAN assignment to users.
D. RADIUS can send a DO-NOT-AUTHORIZE demand to the authenticator to prevent the STA from gaining access to specific files, but may only employ this in relation to Linux servers.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30 Role-Based Access Control (RBAC) allows a WLAN administrator to perform what network function?

A. Provide two or more user groups connected to the same SSID with different levels of network privileges.
B. Allow access to specific files and applications based on the user's WMM access category.
C. Allow simultaneous support for multiple EAP types on a single access point.
D. Minimize traffic load on an AP by requiring mandatory admission control for use of the Voice access category.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
A large enterprise is designing a secure, scalable, and manageable 802.11n WLAN that will support thousands of users. The enterprise will support both 802.1X/EAP-TTLS and PEAPv0/MSCHAPv2. Currently, the company is upgrading network servers as well and will replace their existing Microsoft IAS implementation with Microsoft NPS, querying Active Directory for user authentication. For this organization, as they update their WLAN infrastructure, what WLAN controller feature will likely be least valuable?

A. SNMPv3 support
B. 802.1Q VLAN trunking
C. Internal RADIUS server
D. WIPS support and integration
E. WPA2-Enterprise authentication/encryption

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
ABC Company is implementing a secure 802.11 WLAN at their headquarters (HQ) building in New York and at each of the 10 small, remote branch offices around the United States. 802.1X/EAP is ABC's preferred security solution, where possible. All access points (at the HQ building and all branch offices) connect to a single WLAN controller located at HQ. Each branch office has only a single AP and minimal IT resources. What security best practices should be followed in this deployment scenario?

A. Remote management of the WLAN controller via Telnet, SSH, HTTP, and HTTPS should be prohibited across the WAN link.
B. RADIUS services should be provided at branch offices so that authentication server and suppliant credentials are not sent over the Internet.
C. An encrypted VPN should connect the WLAN controller and each remote controller-based AP, or each remote site should provide an encrypted VPN tunnel to HQ.
D. APs at HQ and at each branch office should not broadcast the same SSID; instead each branch should have a unique ID for user accounting purposes.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
ABC Company is an Internet Service Provider with thousands of customers. ABC's customers are given login credentials for network access when they become a customer. ABC uses an LDAP server as the central user credential database. ABC is extending their service to existing customers in some public access areas and would like to use their existing database for authentication. How can ABC Company use their existing user database for wireless user authentication as they implement a large-scale WPA2-Enterprise WLAN security solution?

A. Implement a RADIUS server and query user authentication requests through the LDAP server.
B. Mirror the LDAP server to a RADIUS database within a WLAN controller and perform daily backups to synchronize the user databases.
C. Import all users from the LDAP server into a RADIUS server with an LDAP-to-RADIUS conversion tool.

D. Implement an X.509 compliant Certificate Authority and enable SSL queries on the LDAP server.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
ABC Company has recently installed a WLAN controller and configured it to support WPA2-Enterprise security. The administrator has configured a security profile on the WLAN controller for each group within the company (Marketing, Sales, and Engineering). How are authenticated users assigned to groups so that they receive the correct security profile within the WLAN controller?

A. The RADIUS server sends the list of authenticated users and groups to the WLAN controller as part of a 4-Way Handshake prior to user authentication.
B. The WLAN controller polls the RADIUS server for a complete list of authenticated users and groups after each user authentication.
C. The RADIUS server sends a group name return list attribute to the WLAN controller during every successful user authentication.
D. The RADIUS server forwards the request for a group attribute to an LDAP database service, and LDAP sends the group attribute to the WLAN controller.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
ABC Company is deploying an IEEE 802.11-compliant wireless security solution using 802.1X/EAP authentication. According to company policy, the security solution must prevent an eavesdropper from decrypting data frames traversing a wireless connection. What security characteristic and/or component plays a role in preventing data decryption?

A. 4-Way Handshake
B. PLCP Cyclic Redundancy Check (CRC)
C. Multi-factor authentication
D. Encrypted Passphrase Protocol (EPP)
E. Integrity Check Value (ICV)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36 The IEEE 802.11 Pairwise Transient Key (PTK) is derived from what cryptographic element?

A. PeerKey (PK)
B. Group Master Key (GMK)
C. Key Confirmation Key (KCK)
D. Pairwise Master Key (PMK)
E. Phase Shift Key (PSK)
F. Group Temporal Key (GTK)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
In the basic 4-way handshake used in secure 802.11 networks, what is the purpose of the ANonce and SNonce?

A. They are added together and used as the GMK, from which the GTK is derived.
B. They are used to pad Message 1 and Message 2 so each frame contains the same number of bytes.
C. The IEEE 802.11 standard requires that all encrypted frames contain a nonce to serve as a Message Integrity Check (MIC).
D. They are input values used in the derivation of the Pairwise Transient Key.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
ABC Company has a WLAN controller using WPA2-Enterprise with PEAPv0/MS-CHAPv2 and AES-CCMP to secure their corporate wireless data. They wish to implement a guest WLAN for guest users to have Internet access, but want to implement some security controls. The security requirements for the hotspot include:

- Cannot access corporate network resources
- Network permissions are limited to Internet access
- All stations must be authenticated

What security controls would you suggest? (Choose the single best answer.)

A. Configure access control lists (ACLs) on the guest WLAN to control data types and destinations.
B. Require guest users to authenticate via a captive portal HTTPS login page and place the guest WLAN and the corporate WLAN on different VLANs.
C. Implement separate controllers for the corporate and guest WLANs.
D. Use a WIPS to deauthenticate guest users when their station tries to associate with the corporate WLAN.
E. Force all guest users to use a common VPN protocol to connect.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39 The IEEE 802.11 standard defined Open System authentication as consisting of two auth frames and two assoc frames. In a WPA2-Enterprise network, what process immediately follows the 802.11 association procedure?

A. 802.1X/ EAP authentication
B. Group Key Handshake
C. DHCP Discovery
D. RADIUS shared secret lookup
E. 4-Way Handshake
F. Passphrase-to-PSK mapping

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Your company has just completed installation of an IEEE 802.11 WLAN controller with 20 controller-based APs. The CSO has specified PEAPv0/EAP-MSCHAPv2 as the only authorized WLAN authentication mechanism. Since an LDAPcompliant user database was already in use, a RADIUS server was installed and is querying authentication requests to the LDAP server. Where must the X.509 server certificate and private key be installed in this network?

A. Controller-based APs
B. WLAN controller
C. RADIUS server
D. Supplicant devices
E. LDAP server

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
You support a coffee shop and have recently installed a free 802.11ac wireless hotspot for the benefit of your customers. You want to minimize legal risk in the event that the hotspot is used for illegal Internet activity. What option specifies the best approach to minimize legal risk at this public hotspot while maintaining an open venue for customer Internet access?

A. Require client STAs to have updated firewall and antivirus software.
B. Block TCP port 25 and 80 outbound on the Internet router.
C. Use a WIPS to monitor all traffic and deauthenticate malicious stations.
D. Implement a captive portal with an acceptable use disclaimer.
E. Allow only trusted patrons to use the WLAN.
F. Configure WPA2-Enterprise security on the access point.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
You are using a utility that takes input and generates random output. For example, you can provide the input of a known word as a secret word and then also provide another known word as salt input. When you process the input it generates a secret code which is a combination of letters and numbers with case sensitivity. For what is the described utility used?

A. Generating PMKs that can be imported into 802.11 RSN-compatible devices.
B. Generating passwords for WLAN infrastructure equipment logins.
C. Generating dynamic session keys used for IPSec VPNs.
D. Generating GTKs for broadcast traffic encryption.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Many corporations configure guest VLANs on their WLAN controllers that allow visitors to have Internet access only. The guest traffic is tunneled to the DMZ to prevent some security risks. In this deployment, what risk is still associated with implementing the guest VLAN without any advanced traffic monitoring or filtering feature enabled?

A. Intruders can send spam to the Internet through the guest VLAN.
B. Peer-to-peer attacks can still be conducted between guest users unless application-layer monitoring and filtering are implemented.
C. Guest users can reconfigure AP radios servicing the guest VLAN unless unsecure network management protocols (e.g. Telnet, HTTP) are blocked.
D. Once guest users are associated to the WLAN, they can capture 802.11 frames from the corporate VLANs.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
While seeking the source of interference on channel 11 in your 802.11n WLAN running within 2.4 GHz, you notice a signal in the spectrum analyzer real time FFT display. The signal is characterized with the greatest strength utilizing only 12 megahertz of bandwidth and it does not use significantly more bandwidth until it has weakened by roughly 20 dB. At approximately -70 dB, it spreads across as much as 35 megahertz of bandwidth. What kind of signal is described?

A. A high-power ultra wideband (UWB) Bluetooth transmission.
B. A 2.4 GHz WLAN transmission using transmit beam forming.
C. A high-power, narrowband signal.
D. A deauthentication flood from a WIPS blocking an AP.
E. An HT-OFDM access point.
F. A frequency hopping wireless device in discovery mode.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
The Marketing department's WLAN users need to reach their file and email server as well as the Internet, but should not have access to any other network resources. What single WLAN security feature should be implemented to comply with these requirements?

A. RADIUS policy accounting
B. Group authentication
C. Role-based access control
D. Captive portal
E. Mutual authentication

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
XYZ Hospital plans to improve the security and performance of their Voice over Wi-Fi implementation and will be upgrading to 802.11n phones with 802.1X/EAP authentication. XYZ would like to support fast secure roaming for the phones and will require the ability to troubleshoot reassociations that are delayed or dropped during inter-channel roaming. What portable solution would be recommended for XYZ to troubleshoot roaming problems?

A. Spectrum analyzer software installed on a laptop computer.
B. An autonomous AP mounted on a mobile cart and configured to operate in monitor mode.
C. Laptop-based protocol analyzer with multiple 802.11n adapters.
D. WIPS sensor software installed on a laptop computer.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47 For which one of the following purposes would a WIPS not be a good solution?

A. Enforcing wireless network security policy.
B. Detecting and defending against eavesdropping attacks.
C. Performance monitoring and troubleshooting.
D. Security monitoring and notification.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
For a WIPS system to identify the location of a rogue WLAN device using location pattering (RF fingerprinting), what must be done as part of the WIPS installation?

A. A location chipset (GPS) must be installed with it.
B. At least six antennas must be installed in each sector.
C. The RF environment must be sampled during an RF calibration process.
D. All WIPS sensors must be installed as dual-purpose (AP/sensor) devices.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
A network security auditor is preparing to perform a comprehensive assessment of an 802.11ac network's security. What task should be performed at the beginning of the audit to maximize the auditor's ability to expose network vulnerabilities?

A. Identify the IP subnet information for each network segment.
B. Identify the manufacturer of the wireless infrastructure hardware.
C. Identify the skill level of the wireless network security administrator(s).
D. Identify the manufacturer of the wireless intrusion prevention system.
E. Identify the wireless security solution(s) currently in use.

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
Joe's new laptop is experiencing difficulty connecting to ABC Company's 802.11 WLAN using 802.1X/EAP PEAPv0. The company's wireless network administrator assured Joe that his laptop was authorized in the WIPS management console for connectivity to ABC's network before it was given to him. The WIPS termination policy includes alarms for rogue stations, rogue APs, DoS attacks and unauthorized roaming. What is a likely reason that Joe cannot connect to the network?

A. An ASLEAP attack has been detected on APs to which Joe's laptop was trying to associate. The WIPS responded by disabling the APs.
B. Joe configured his 802.11 radio card to transmit at 100 mW to increase his SNR. The WIPS is detecting this much output power as a DoS attack.
C. Joe's integrated 802.11 radio is sending multiple Probe Request frames on each channel.
D. Joe disabled his laptop's integrated 802.11 radio and is using a personal PC card radio with a different chipset, drivers, and client utilities.

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
The following numbered items show some of the contents of each of the four frames exchanged during the 4-way handshake.

1. Encrypted GTK sent
2. Confirmation of temporal key installation
3. ANonce sent from authenticator to supplicant
4. SNonce sent from supplicant to authenticator, MIC included

Arrange the frames in the correct sequence beginning with the start of the 4-way handshake.

A. 1, 2, 3, 4 B.
3, 4, 1, 2 C. 4,
3, 1, 2
D. 2, 3, 4, 1

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
You are the WLAN administrator in your organization and you are required to monitor the network and ensure all active WLANs are providing RSNs. You have a laptop protocol analyzer configured. In what frame could you see the existence or non-existence of proper RSN configuration parameters for each BSS through the RSN IE?

A. CTS
B. Beacon
C. RTS
D. Data frames
E. Probe request

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53 What attack cannot be detected by a Wireless Intrusion Prevention System (WIPS)?

A. Deauthentication flood
B. Soft AP
C. EAP flood
D. Eavesdropping
E. MAC Spoofing
F. Hotspotter

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54 What security vulnerability may result from a lack of staging, change management, and installation procedures for WLAN infrastructure equipment?

A. The WLAN system may be open to RF Denial-of-Service attacks.
B. Authentication cracking of 64-bit Hex WPA-Personal PSK.
C. AES-CCMP encryption keys may be decrypted.
D. WIPS may not classify authorized, rogue, and neighbor APs accurately.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55 What field in the RSN information element (IE) will indicate whether PSK- or Enterprise-based WPA or WPA2 is in use?

A. Group Cipher Suite
B. Pairwise Cipher Suite List
C. AKM Suite List
D. RSN Capabilities

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56 What preventative measures are performed by a WIPS against intrusions?

A. Uses SNMP to disable the switch port to which rogue APs connect.
B. Evil twin attack against a rogue AP.
C. EAPoL Reject frame flood against a rogue AP.
D. Deauthentication attack against a classified neighbor AP.
E. ASLEAP attack against a rogue AP.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 57 When monitoring APs within a LAN using a Wireless Network Management System (WNMS), what secure protocol may be used by the WNMS to issue configuration changes to APs?

A. PPTP
B. 802.1X/EAP
C. TFTP
D. SNMPv3
E. IPSec/ESP

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 58 WLAN protocol analyzers can read and record many wireless frame parameters. What parameter is needed to physically locate rogue APs with a protocol analyzer?

A. IP Address
B. Noise floor
C. RSN IE
D. SSID
E. Signal strength
F. BSSID

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
After completing the installation of a new overlay WIPS for the purpose of rogue detection and security monitoring at your corporate headquarters, what baseline function MUST be performed in order to identify the security threats?

A. Separate security profiles must be defined for network operation in different regulatory domains.
B. WLAN devices that are discovered must be classified (rogue, authorized, neighbor, etc.) and a WLAN policy must define how to classify new devices.
C. Upstream and downstream throughput thresholds must be specified to ensure that service-level agreements are being met.
D. Authorized PEAP usernames must be added to the WIPS server's user database.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60 A WLAN protocol analyzer trace reveals the following sequence of frames (excluding the ACK frames):

1. 802.11 Probe Req and 802.11 Probe Rsp
2. 802.11 Auth and then another 802.11 Auth
3. 802.11 Assoc Req and 802.11 Assoc Rsp
4. EAPOL-KEY
5. EAPOL-KEY
6. EAPOL-KEY
7. EAPOL-KEY

What security mechanism is being used on the WLAN?

A. WPA2-Personal
B. 802.1X/LEAP
C. EAP-TLS
D. WPA-EnterpriseE. WEP-128

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference: